

### REMARKS/ARGUMENTS

Claims 35-58 are pending. An Office Action mailed July 26, 2005 rejects claims 35, 37-42, 44-49, and 51-55 under 35 U.S.C. §103 as obvious over Gifford (U.S. Pat. 6,205,437) in view of Bishop (U.S. Pub. 2004/0243520) and Shwartz (U.S. Pub. 2001/0044787), and rejects claims 36, 43, and 50 under §103 as obvious over Gifford, Bishop, Shwartz, and Baltzley (U.S. Pub. 2001/0014158). These rejections stand affirmed by a Decision of the Board of Patent Appeals and Interferences mailed March 25, 2008. By this Amendment, claims 35, 40, 42, 47, 49, and 54 are amended and claims 56-58 are new. No new matter has been added.

#### 35 U.S.C. §103 Rejections

As set out in the BPAI decision, Gifford discloses a method of authenticating a payment transaction over a network in which the payment order is checked for replay (i.e., repetition) by associating a nonce with each payment order. Bishop discloses a similar method for authenticating a payment transaction using a challenge-response system, where the user's response is authenticated with a smart card. Shwartz discloses a method of authenticating a payment transaction in which, as interpreted by the Board, a request for approval of the transaction is sent in the challenge-response.

However, none of the references describe a system that verifies both (1) that the buyer intends to make the designated purchase and (2) that **the buyer is authorized** to use the designated payment instrument.

Claim 1 is exemplary and recites, in relevant part:

at a payment authorization service, storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

linking the PKI key pair to at least **a first payment instrument of a buyer**;

in response to receiving a challenge response from the buyer over the network...determining that the buyer has access to the private key and that

**the buyer is authorized to use the first payment instrument by using the public key to decrypt the digitally signed summary of the payment transaction; and**

**sending an authentication response to the seller over the network, the authentication response including an indication that the buyer is authorized to use the first payment instrument.**

Insofar as the cited references describe payment instruments, it is only to mention that a buyer can specify the payment instrument used in a transaction (e.g., Gifford col. 5, FIG. 4). There is no description or suggestion of an authentication response sent to a seller that includes an indication that a buyer is authorized to use a particular payment instrument. Further, Gifford's "purchase authorization" (e.g., 28, 55 in FIGS. 6, 12) merely verifies that a buyer has sufficient funds and that a shipping address is valid (*see* col. 8:12-24, FIG. 13); there is no suggestion of verifying that a user is authorized to use a specific payment instrument by decrypting a digitally-signed payment transaction summary. Similarly, the other cited references fail to describe verifying that a buyer is authorized to use a payment instrument, and specifically verifying that a buyer is authorized to use a payment instrument by decrypting a digitally-signed payment transaction summary as required by the claims. For at least this reason, the claims are not obvious over the cited art.

Further, none of the references describe a buyer profile as recited in the claims. For example, claim 40 recites, in relevant part:

**a buyer profile...linked to the PKI key pair and including a plurality of payment instruments** and a plurality of shipping addresses;

Claim 54 recites similar features. None of the cited references describe such a profile, and specifically they do not describe or suggest linking a buyer profile with multiple payment options to the buyer's PKI certificate. Where multiple shipping addresses are used (e.g., Gifford col. 8), they are maintained as a list of approved destination addresses in a database; there is no suggestion that they are linked to a PKI key pair associated with the buyer that is used to encrypt payment transaction summaries. The references only refer to "multiple" payment sources by

suggesting that buyers may use different **types** of funds, such as Visa, Mastercard, e-check, etc. *See, e.g.*, Gifford, FIG. 4 and col. 5:32-36 (indicating that the user must enter an account number for each transaction). They do not suggest linking multiple specific payment instruments to a buyer's PKI credentials. For at least these reasons, claims 40 and 54 are patentable over the cited references.

### CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 202-481-9900.

Respectfully submitted,

/ASKamlay/  
Aaron S Kamlay  
Reg. No. 58813

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 202-481-9900  
Fax: 415-576-0300  
61370928 v1